

FILED

SEP 09 2024

PETER A. MOORE, JR., CLERK
BY US DISTRICT COURT, EDNC
86 DEP CLK

UNITED STATES DISTRICT COURT
for the
Eastern District of North Carolina

IN THE MATTER OF THE SEARCH OF:
FILES CONTAINED WITHIN THE NCMEC
CYBERTIPLINE REPORT 175154617
CURRENTLY IN THE CUSTODY OF THE
ARMED FORCES INTERNET CRIMES
AGAINST CHILDREN (ICAC) TASK
FORCE AND MORE FULLY DESCRIBED
IN ATTACHMENT A, ATTACHED
HERETO.

Case No. 7:24-mj-1206-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

As described in Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized). See Attachment B hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

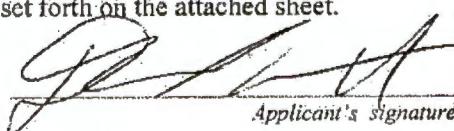
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A	Distribution, Receipt, and/or Possession Child Pornography

The application is based on these facts:

See attached affidavit which is attached hereto and incorporated herein by reference

Continued on the attached sheet;

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Daniel Ott

Printed name and title

On this day, Daniel Ott
appeared before me via reliable electronic means, was
placed under oath, and attested to the contents of this
Application for a Search Warrant.

Date: September 9 2024


Judge's signature

Robert B. Jones, Jr. United States Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH
OF FILES CONTAINED WITHIN
THE NCMEC CYBERTIPLINE
REPORT 175154617 CURRENTLY
IN THE CUSTODY OF THE
ARMED FORCES INTERNET
CRIMES AGAINST CHILDREN
(ICAC) TASK FORCE AND MORE
FULLY DESCRIBED IN
ATTACHMENT A, ATTACHED
HERETO.

Case No. 7:24-mj-1206-RJ

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Ott (Your Affiant), Special Agent with the United States Naval Criminal Investigative Service Resident Agency (NCISRA), Camp Lejeune, North Carolina (CLNC), being first duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief.

INTRODUCTION

1. Based on my training and experience and the facts set forth in this affidavit, Your Affiant submits there is probable cause to believe that violations of Title 18, United States Code, Section 2252A (Possession of Child Sexual Abuse Material (CSAM)) have occurred. Furthermore, there is also probable cause to search the locations described in Attachment A for evidence of these crimes and seize the information described in Attachment B.

Page 1 of 13

CLW

2. This affidavit is based upon the investigative efforts by Your Affiant as well as other NCIS Agents and Law Enforcement Members. Since this affidavit is being submitted for the limited purpose of securing a Search Warrant, Your Affiant has not included each and every finding from the investigation; rather, Your Affiant has set forth a summary of the investigation to date in order to establish probable cause that evidence, fruits, and instrumentalities of said violations are contained in the location described in Attachment A.

3. I have been assigned as a Special Agent to the U.S. Naval Criminal Investigative Service (NCIS) since October 2023. Your Affiant is currently assigned to the General Crimes Squad, Camp Lejeune, NC. Your Affiant is routinely tasked to investigate violations of the Uniform Code of Military Justice (UCMJ) and Federal crimes. These types of violations include crimes of violence, child sexual and physical abuse, and crimes related to child exploitation and child pornography, including the illegal production, distribution, receipt, and possession of child pornography.

4. I have completed the five-month Special Agent Basic Training Integrated (SABTI) at the Federal Law Enforcement Training Center in Glynco, GA. These programs provided me with instruction regarding death investigations, sex crimes investigations, narcotics investigations, military law, civilian federal law, and other practical issues for investigators. I have participated in a number of investigations as a Federal Special Agent. During these investigations, I have conducted interviews and other follow-up investigative endeavors including cases

involving the investigation of child sexual abuse and child pornography. Your Affiant has been in the Law Enforcement Career Field since 2019 and possess a Bachelor's Degree in Engineering from the Pennsylvania State University.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(1) prohibits any person from knowingly transports or ships, using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer child pornography.

b. Title 18, United States Code, Sections 2252A(a)(2)(A) prohibits any person from knowingly receives or distributes any child pornography using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, United States Code, Sections 2252A(a)(2)(B) prohibits any person from knowingly receiving or distributing material that contains child pornography using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits any person from knowingly possessing or accessing with the intent to view, any book,

magazines, periodicals, films, video tapes, or any other material that contains an image of child pornography that has been mailed, or shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:
 - a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

CYBERTIPLINE REPORTS

7. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children and

serves as a repository for information about child pornography. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers ("ESP") to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The Electronic Service Provider submits the report and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The Electronic Service Provider may or may not independently view the content of the file(s) it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the Electronic Service Provider submits, such as IP addresses. NCMEC then packages the information from the Electronic Service Provider along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred.

PROBABLE CAUSE STATEMENT

8. On or about September 28th, 2023, the Electronic Service Provider (ESP), Google, Inc., submitted CyberTipline Report 175154617 to NCMEC. As reported by

the ESP, the incident included forty-nine (49) uploaded files, the incident type was: Apparent Child Pornography (possession, manufacture, and distribution), and the incident date and time were listed as: September 27th, 2023, 20:12:32 UTC. Furthermore, the CyberTip listed the incident type as: Apparent Child Pornography and noted the Report contained a "Hash Match."

9. The report indicated the ESP reviewed the contents of eight (8) of the file(s) and verified the eight (8) files as Apparent Child Pornography. The ESP reported the uploads were associated with the following additional information: Full name: "Andrew Tarleton," email address "andytarleton@gmail.com," phone number +2075040519, date of birth 02-11-1993. The ESP additionally provided multiple Internet Protocol (IP) addresses associated with the Google user's upload and/or login dates, as early as January 02, 2023, and as recent as September 27, 2023.

10. NCMEC then used publicly available search tools to query the IP addresses and determined more than one (1) IP address resolved to Jacksonville, NC. NCMEC additionally conducted a query of the phone number provided by the ESP, +2075040519, which resolved to Spectrum. Upon receipt of the CyberTip, I conducted an additional query of the aforementioned phone number and identified GySgt Andrew TARLETON, USMC, 1st Battalion, 2nd Marines, 2nd Marine Division, as being associated with the phone number. Law enforcement queries confirmed TARLETON is an Active-Duty Marine stationed at Camp Lejeune, NC. I currently have access to the CyberTipline Report and the contents of the file the ESP uploaded in connection with the CyberTip through the ICAC Data System (IDS).

11. I know from my training and experience the ESP flags and reports images or files that have the same "hash values" as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is akin to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value—the hash value—is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

12. Here, I know from my training and experience the ESP compares the hash values of files that its customers transmit on its systems against the list of hash values the Armed Forces Internet Crimes Against Children (ICAC) Task Force has. If the ESP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ESP's systems.

13. On 12Aug24, I reviewed the eight (8) files of suspected child pornography provided to NCIS from the NCMEC. Seven (7) of the images are apparent child pornography and one (1) image is suspected to be child pornography. The following is a brief description of three (3) of the images

(a) Title: 15c95b53d6251506696f7db1bb351613-20170912082039.jpg.

Image File: This frontal image depicts a pre-pubescent female approximately six (6) years of age. The female's full body is in the image in which she is completely nude

exposing her breasts and vagina. The female is sitting down on what appears to be a sheet on the edge of a bed.

(b) Title: 6f3b7d448897c0472c42e13ba2f6284-uc9ypb099v.giv. Video Duration: 00:06 Seconds. Description: The video file depicts a prepubescent female appearing to be between five (5) and six (6) years old, wearing a red t-shirt and no visible clothing from the waist down. The female is leaned back and fondling her exposed vagina in a lewd manner.

(c) Title: 78eb49fbb2b0270c3691783f4b6ae676-LB63598125841.jpg. Image File: This image depicts a prepubescent female lying on her back wearing a pink sweatshirt with no clothing from the waist down. The female is laying on what appears to be blankets with her legs spread and her vagina exposed. The female is looking at the camera and has one finger on her left hand pointing to or touching her lips.

14. Therefore, there is probable cause to believe the remaining unviewed forty-one (41) files that the ESP reported in connection with the submitted CyberTipline Report 175154617 contains child pornography.

LEGAL AUTHORITY

14. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled, "stored wire and electronic communications and transactional records access."

15. Title 18 United States Code 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant

to 18 U.S.C. § 2703, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction.

16. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of North Carolina because IP subscriber information indicated that the subject of the CyberTipline Report 165663259, uses the account from an address within the Eastern District of North Carolina. See 18 U.S.C. § 3237(a); see also 18 U.S.C. §§ 3231 and 3232.

CONCLUSION

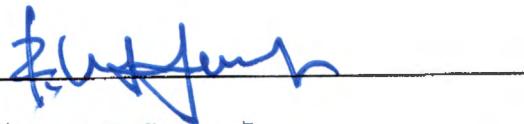
17. Based on the investigation described above, probable cause exists to believe inside the file the ESP uploaded in connection with the above CyberTipline Report (described in Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 2252A(a)(1), (2), (3), (4) and (5) (described in Attachment B).

18. I, therefore, respectfully request that that attached warrant be issued authorizing the search and seizure of the items described in **Attachment A** and listed in **Attachment B**.



Daniel Ott, Special Agent,
Naval Criminal Investigative Service

Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3), this 9 day of September 2024.



Robert B. Jones, Jr.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

Content of file(s) uploaded in connection with CyberTipline Report 175154617 (hereinafter and in Attachment B the "File(s)"), currently held by the Armed Forces Internet Crimes Against Children (ICAC) Task Force at 27130 Telegraph Road, Quantico, VA 22134.

CyberTip Report	Number of files contained in the report that were uploaded by the user:
175154617	49

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

For the File(s) listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(1), (2), (3), (4), and (5):

1. Images or visual depictions of child pornography.
2. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors.
3. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the File(s), or that aid in the identification of persons involved in violations of 18 U.S.C. Sections 2252A(a)(1), (2), (3), (4), and (5).

DEFINITIONS

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer data or electronic storage; any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as digital image files; microfilm,

microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. "Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.
6. "Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).